Homeland Security Presidential Directive/HSPD-12

Policy for a Common Identification Standard for Federal Employees and Contractors

In response to HSPD 12 (which directed the Secretary of Commerce to "promulgate in accordance with applicable laws a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive") , the NIST Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. Federal Information Processing Standard (FIPS) 201, entitled *Personal Identity Verification of Federal Employees and Contractors*, was developed to satisfy the requirements of HSPD 12, approved by the Secretary of Commerce, and issued on February 25, 2005.

FIPS 201 incorporates three technical publications specifying several aspects of the required administrative procedures and technical specifications that may change as the standard is implemented and used. NIST Special Publication 800-73, "Interfaces for Personal Identity Verification" specifies the interface and data elements of the PIV card; NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification" specifies the technical acquisition and formatting requirements for biometric data of the PIV system; and NIST Special Publication 800-78, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification" specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system.

In addition, a number of guidelines, reference implementations, and conformance tests have been identified as being needed to: implement and use the PIV system; protect the personal privacy of all subscribers of the PIV system; authenticate identity source documents to obtain the correct legal name of the person applying for a PIV "card"; electronically obtain and store required biometric data (e.g., fingerprints, facial images) from the PIV system subscriber; create a PIV "card" that is "personalized" with data needed by the PIV system to later grant access to the subscriber to Federal facilities and information systems; assure appropriate levels of security for all applicable Federal applications; and provide interoperability among Federal organizations using the standards.

See http://csrc.nist.gov/piv-program/index.html